CFCA 证书工具包（Ultimate 版）

接口使用手册

中国金融认证中心

2017 年 05 月 9 日

文档修订记录

本文档会随时保持更新，请与中国金融认证中心索要最新版本

版本	内容	日期	编写	审核
3.0	2.2.2 GetSignCertInfo、2.4.2 GetEncrypCertInfo 接口增加获取颁发者 DN 功能	2014/07/22	姜景竹	
3.1	数字信封操作相关接口，新增对国密新标准（C1||C3||C2）的支持	2014/08/28	张欣欣	秘相友
3.2	支持国密非注册证书	2016/12/21	张欣欣	
3.3	SM2 数字信封解密时去除对证书唯一性的检查	2017/05/09	胡军华	张欣欣

注：对该文件内容增加、删除或修改须填写此修订记录，详细记载变更信息，以保证其可追溯性。

目录

1 文档描述

该文档主要描述 SM2 证书工具包的运行环境、接口定义以及调用方式。示例 demo 为 HTML 语言编写。

2 运行环境

2.1 语言显示

页面语言环境支持：美国英文及简体中文

2.2 操作系统

- 32 位操作系统

Windows XP、Windows Vista、Windows 7、Windows 8、WinServer2003、WinServer2008

- 64 位操作系统

Windows Vista、Windows 7、Windows 8、WinServer2003、WinServer2008

- IE 浏览器

IE6、IE7、IE8、IE9、IE10、IE11

- 非 IE 浏览器

Chrome 12.0-44.0、Firefox 4.0-Firefox43.0、Safari 5.0-5.1.7、Opera 11.0-12.15

2.3 提供版本

提供 IE 的 32 位和 64 位的 cab，exe，非 IE 的 exe。

3 功能描述

3.1 消息的签名与验签

3.1.1 SelectCertificate

HRESULT SelectCertificate(BSTR bstrSubjectDNFilter,BSTR bstrIssuerDNFilter, BSTR bstrSerialNumFilter , VARIANT_BOOL* pbSuccess)

描述:

通过传入的字符串作为 DN 的筛选条件，选择出符合 DN 条件的带私钥的 SM2/RSA 签名证书。如果筛选字符串为空，则对相应条件不进行筛选。

其中 SM2 证书仅支持非注册的。

如需选择 SM2 证书，在调用此接口前必须至少调用一次 SetSM2CSPList 接口。

参数:

BSTR bstrSubjectDNFilter: [IN]目标证书主题 DN 中所包含的字符串，作为该筛选条件选出证书。

BSTR bstrIssuerDNFilter: [IN]目标证书颁发者 DN 中所包含的字符串，作为该

筛选条件选出证书。

BSTR bstrSerialNumFilter: [IN]目标证书的序列号，作为该筛选条件选出证书。

VARIANT_BOOL* pbSuccess: [OUT， RETVAL] 成功返回 VARIANT_TRUE，否则返回 VARIANT_FALSE。

3.1.2 GetSignCertInfo

HRESULT GetSignCertInfo（BSTR bstrInfoType,BSTR* pbstrInfoContent）

描述:

根据传入的标识，获得已选定证书（通过 SelectCertificate 选定的证书）的相关信息。

参数:

BSTR bstrInfoType: [IN]要获取的信息类型标识（不区分大小写）。

“SubjectDN”： 证书主题 DN；

“SubjectCN”： 证书主题 CN；

“SerialNumber”： 证书序列号；

“CSPName”： 证书对应的 CSP 名称；

“CertType”： 证书类型；SM2 或 RSA。

“IssuerDN”： 颁发者 DN。

BSTR* pbstrInfoContent: [OUT， RETVAL] 成功返回获取到的信息，失败返回

空。

3.1.3 SignMsgPKCS1

HRESULT SignMsgPKCS1（BSTR bstrSourceData, BSTR bstrHashAlg, BSTR* pbstrSignature）

描述:

对字符串进行 SM2/RSA 签名，返回 Base64 编码的裸 SM2/RSA 签名结果（相当于 PKCS#1）；其中 RSA 签名可以使用 SHA-1 或 SHA-256 计算哈希值，SM2 签名使用 SM3 计算哈希值。

参数:

BSTR bstrSourceData: [IN] 待签名的字符串，签名之前控件会将其转换为 UTF-8 编码。

BSTR bstrHashAlg:[IN] 使用 RSA 签名的算法。传入“SHA-1”、“SHA-256”“SHA-384”，“SHA-512”，不区分大小写。

BSTR* pbstrSignature: [OUT，RETVAL] Base64 编码的裸 SM2/RSA 签名结果（相当于 PKCS#1）。

3.1.4 SignMsgPKCS7

HRESULT SignMsgPKCS7（BSTR bstrSourceData, BSTR bstrHashAlg,

VARIANT_BOOL bWithSourceData, BSTR* pbstrSignature）

描述:

对字符串进行 SM2/RSA 签名，返回 Base64 编码的 PKCS#7 签名结果。

参数:

BSTR bstrSourceData: [IN] 待签名的字符串，签名之前控件会将其转换为 UTF-8 编码。

BSTR bstrHashAlg:[IN] 使用 RSA 签名的算法。传入“SHA-1”、“SHA-256”“SHA-384”，“SHA-512”，不区分大小写。

VARIANT_BOOL bWithSourceData: [IN] 签名结果是否带原文。

VARIANT_TRUE: 带原文；VARIANT_FALSE: 不带原文。

BSTR* pbstrSignature: [OUT，RETVAL] Base64 编码的 PKCS#7 签名结果。

3.1.5 SignMsgPKCS1_BySoftCert

HRESULT SignMsgPKCS1_BySoftCert （ BSTR bstrSoftCertFileName, BSTR bstrSoftCertPassword, BSTR bstrSoftCertType,BSTR bstrSourceData, BSTR bstrHashAlg, BSTR* pbstrSignature）

描述:

用传入的 SM2/PFX 文件证书对字符串进行 SM2/RSA 签名，返回 Base64 编码的裸 SM2/RSA 签名结果（相当于 PKCS#1）。

参数:

BSTR bstrSoftCertFileName: [IN] 用于签名的 SM2/PFX 文件证书的路径。

BSTR bstrSoftCertPassword: [IN] 用于签名的 SM2/PFX 文件证书的密码。

BSTR bstrSoftCertType:[IN] 用于签名证书文件类型。SM2 文件、PFX 文件。

BSTR bstrSourceData: [IN] 待签名的字符串，签名之前控件会将其转换为 UTF-8 编码。

BSTR bstrHashAlg:[IN] 使用 RSA 签名的算法。传入“SHA-1”、“SHA-256”“SHA-384”，“SHA-512”，不区分大小写。

BSTR * pbstrSignature: [OUT， RETVAL] Base64 编码的 PKCS#1 签名值。

3.1.6 SignMsgPKCS7_BySoftCert

HRESULT SignMsgPKCS7_BySoftCert （ BSTR bstrSoftCertFileName, BSTR bstrSoftCertPassword, BSTR bstrSoftCertType,BSTR bstrSourceData, BSTR bstrHashAlg, VARIANT_BOOL bWithSourceData,BSTR* pbstrSignature）

描述:

用传入的 SM2/PFX 文件证书对字符串进行 PKCS#7 签名。

参数:

BSTR bstrSoftCertFileName: [IN] 用于签名的 SM2/PFX 文件证书的路径。

BSTR bstrSoftCertPassword: [IN] 用于签名的 SM2/PFX 文件证书的密码。

BSTR bstrSoftCertType:[IN] 用于签名证书文件类型。SM2 文件、PFX 文件。

BSTR bstrSourceData: [IN] 待签名的字符串，签名之前控件会将其转换为 UTF-8 编码。

BSTR bstrHashAlg:[IN] 使用 RSA 签名的算法。传入“SHA-1”、“SHA-256”“SHA-384”，“SHA-512”，不区分大小写。

VARIANT_BOOL bWithSourceData: [IN] 签名是否带原文，VARIANT_TRUE: 带原文，VARIANT_FALSE: 不带原文。

BSTR * pbstrSignature: [OUT， RETVAL] Base64 编码的 PKCS#7 签名值。

3.1.7 VerifyMsgSignaturePKCS1

HRESULT VerifyMsgSignaturePKCS1 （ BSTR bstrSignature, BSTR bstrSignatureType,BSTR bstrSourceMsg, BSTR bstrHashAlg, BSTR bstrBase64CertContent,VARIANT_BOOL* pbSuccess）

描述:

对裸 SM2/RSA 签名结果（相当于 PKCS#1）进行验签。

参数:

BSTR bstrSignature: [IN] Base64 编码的裸 SM2 签名结果（相当于 PKCS#1）。

BSTR bstrSignatureType:[IN]签名类型。SM2、RSA 算法。

BSTR bstrSourceMsg: [IN]消息原文。

BSTR bstrHashAlg:[IN] 使用 RSA 签名的算法。传入“SHA-1”、“SHA-256”“SHA-384”，“SHA-512”，不区分大小写。

BSTR bstrBase64CertContent: [IN] SM2/RSA 公钥证书，该证书需采用 Base64 编码。

VARIANT_BOOL* pbSuccess: [OUT，RETVAL] 验签结果，VARIANT_TRUE: 成功，VARIANT_FALSE: 失败。

3.1.8 VerifyMsgSignaturePKCS7Attached

HRESULT VerifyMsgSignaturePKCS7Attached （ BSTR bstrSignature, BSTR bstrSignatureType,VARIANT_BOOL* pbSuccess）

描述:

对 SM2/RSA 签名结果进行 PKCS#7 带原文验签。

参数:

BSTR bstrSignature: [IN] Base64 编码的 PKCS#7 带原文签名结果。

BSTR bstrSignatureType:[IN] 签名类型。SM2、RSA 算法。

VARIANT_BOOL* pbSuccess: [OUT，RETVAL] 验签结果，VARIANT_TRUE: 成功，VARIANT_FALSE: 失败。

3.1.9 VerifyMsgSignaturePKCS7Detached

HRESULT VerifyMsgSignaturePKCS7Detached （ BSTR bstrSignature , BSTR bstrSignatureType ,BSTR bstrSourceMsg , VARIANT_BOOL* pbSuccess）

描述:

对 SM2/RSA 签名结果 PKCS#7 不带原文验签。

参数:

BSTR bstrSignature: [IN] Base64 编码的 PKCS#7 不带原文签名结果。

BSTR bstrSignatureType:[IN] 签名类型。SM2、RSA 算法。

BSTR bstrSourceMsg: [IN]消息原文。

VARIANT_BOOL* pbSuccess: [OUT，RETVAL] 验签结果，VARIANT_TRUE: 成功，VARIANT_FALSE: 失败。

3.2 文件的签名与验签

.com、.exe、.bat、.cmd、.vbs、.vbe、.js、.jse、.wsf、.wsh、.msc、.dll 格式文件均不可进行签名及加密操作。

3.2.1 SignFilePKCS1

HRESULT SignFilePKCS1(BSTR bstrSourceFile, BSTR bstrHashAlg, BSTR* pbstrSignature)

描述:

使用 SelectCertificate 选中的证书对文件进行 SM2/RSA 签名，返回 Base64 编码的裸 SM2/RSA 签名结果（相当于 PKCS#1）。

参数:

BSTR bstrSourceFile: [IN] 待签名的文件路径。

BSTR bstrHashAlg:[IN] 使用 RSA 签名的算法。传入“SHA-1”、“SHA-256”“SHA-384”，“SHA-512”，不区分大小写。

BSTR* pbstrSignature: [OUT，RETVAL] Base64 编码的 PKCS#1 签名值。

3.2.2 SignFilePKCS7Detached

HRESULT SignFilePKCS7Detached(BSTR bstrSourceFile, BSTR bstrHashAlg, BSTR* pbstrSignature)

描述:

使用 SelectCertificate 选中的 SM2/RSA 证书对文件进行 PKCS#7 不带原文

签名。

参数:

BSTR bstrSourceFile: [IN] 待签名的文件路径。

BSTR bstrHashAlg:[IN] 使用 RSA 签名的算法。传入“SHA-1”、“SHA-256”“SHA-384”，“SHA-512”，不区分大小写。

BSTR* pbstrSignature: [OUT，RETVAL] Base64 编码的 PKCS#7 签名值。

3.2.3 SignFilePKCS1_BySoftCert

HRESULT SignFilePKCS1_BySoftCert （ BSTR bstrSoftCertFileName, BSTR bstrSoftCertPassword, BSTR bstrSoftCertType, BSTR bstrSourceFile, BSTR bstrHashAlg, BSTR* pbstrSignature）

描述:

用传入的 SM2/RSA 文件证书对文件进行 SM2/RSA 签名，返回 Base64 编码的裸 SM2/RSA 签名结果（相当于 PKCS#1）。

参数:

BSTR bstrSoftCertFileName: [IN] 用于签名的 SM2/PFX 文件证书的路径。

BSTR bstrSoftCertPassword: [IN] 用于签名的 SM2/PFX 文件证书的密码。

BSTR bstrSoftCertType:[IN] 用于签名证书文件类型。SM2 文件、PFX 文件。

BSTR bstrSourceFile: [IN] 待签名文件的路径。

BSTR bstrHashAlg:[IN] 使用 RSA 签名的算法。传入“SHA-1”、“SHA-256”“SHA-384”，“SHA-512”，不区分大小写。

BSTR * pbstrSignature: [OUT，RETVAL] Base64 编码的 PKCS#1 签名值。

3.2.4 SignFilePKCS7Detached_BySoftCert

HRESULT SignFilePKCS7Detached_BySoftCert（BSTR bstrSoftCertFileName, BSTR bstrSoftCertPassword, BSTR bstrSoftCertType, BSTR bstrSourceFile, BSTR bstrHashAlg, BSTR* pbstrSignature）

描述:

用传入的 SM2/PFX 文件证书对文件进行 PKCS#7 不带原文签名。

参数:

BSTR bstrSoftCertFileName: [IN] 用于签名的 SM2/PFX 文件证书的路径。

BSTR bstrSoftCertPassword: [IN] 用于签名的 SM2/PFX 文件证书的密码。

BSTR bstrSoftCertType: [IN] 用于签名证书文件类型。SM2 文件、PFX 文件。

BSTR BSTR bstrSourceFile: [IN] 待签名文件的路径。

BSTR bstrHashAlg:[IN] 使用 RSA 签名的算法。传入“SHA-1”、“SHA-256”“SHA-384”，“SHA-512”，不区分大小写。

BSTR * pbstrSignature: [OUT，RETVAL] Base64 编码的 PKCS#7 签名值。

3.2.5 VerifyFileSignaturePKCS1

HRESULT VerifyFileSignaturePKCS1 （ BSTR bstrSignature, BSTR bstrSignngnatureType,BSTR bstrSourceFile, BSTR bstrHashAlg, BSTR bstrBase64CertContent, VARIANT_BOOL* pbSuccess）

描述:

对 SM2/PFX 文件签名结果（相当于 PKCS#1）进行验签。

参数:

BSTR bstrSignature：[IN] Base64 编码的裸 SM2/PFX 签名结果（相当于 PKCS#1）。

BSTR bstrSignngnatureType:[IN] 签名类型。SM2、RSA 算法。

BSTR bstrSourceFile:[IN] 原文件路径。

BSTR bstrHashAlg:[IN] 使用 RSA 签名的算法。传入“SHA-1”、“SHA-256”“SHA-384”，“SHA-512”，不区分大小写。

BSTR bstrBase64CertContent: [IN] SM2/RSA 公钥证书，该证书需采用 Base64 编码。

VARIANT_BOOL* pbSuccess：[OUT，RETVAL] 验签结果，VARIANT_TRUE：成功，VARIANT_FALSE：失败。

3.2.6 VerifyFileSignaturePKCS7Detached

HRESULT VerifyFileSignaturePKCS7Detached （ BSTR bstrSignature, BSTR bstrSigngnatureType, BSTR bstrSourceFile, VARIANT_BOOL* pbSuccess）

描述:

对 SM2/PFX 文件签名结果进行 PKCS#7 不带原文验签。

参数:

BSTR bstrSignature：[IN] Base64 编码的 PKCS#7 签名结果。

BSTR bstrSigngnatureType:[IN] 签名类型。SM2、RSA 算法。

BSTR bstrSourceFile：[IN] 原文件路径。

VARIANT_BOOL* pbSuccess：[OUT，RETVAL] 验签结果，VARIANT_TRUE：成功，VARIANT_FALSE：失败。

3.3 消息的加密与解密

3.3.1 SelectEncryptCertificate

HRESULT SelectEncryptCertificate （ BSTR bstrSubjectDNFilter, BSTR bstrIssueDNFilter, BSTR bstrSerialNumFilter, BSTR* pbstrSubjectDN）

描述:

按照过滤条件(Subject DN / IssuerDN/ SerialNumber)选择一个用于加密的 SM2/RSA 公钥证书。

其中 SM2 证书仅支持非注册的。

如需选择 SM2 证书，在调用此接口前必须至少调用一次 SetSM2CSPList 接口。

此函数用于基于 USBKey 的加密。

参数:

BSTR bstrSubjectDNFilter: [IN]目标证书中主题 DN 中所包含的字符串，作为该筛选条件选出证书。

BSTR bstrIssueDNFilter: [IN]目标证书中颁发者 DN 中所包含的字符串，作为该筛选条件选出证书。

BSTR bstrSerialNumFilter:[IN]目标证书中证书序列号中所包含的字符串，作为该筛选条件选出证书。

BSTR * pbstrSubjectDN: [OUT，RETVAL] 返回被选出 SM2/RSA 公钥证书的主题 DN。

3.3.2 GetEncrypCertInfo

HRESULT GetEncrypCertInfo（BSTR bstrInfoType, BSTR* pbstrInfoContent）

描述:

根据传入的标识，获得已选定证书（通过 SelectEncryptCertificate 选定

的证书）的相关信息。

参数:

BSTR bstrInfoType: [IN]要获取的信息类型标识（不区分大小写）。

“SubjectDN”： 证书主题 DN；

“SubjectCN”： 证书主题 CN；

“SerialNumber”： 证书序列号；

“CSPName”： 证书对应的 CSP 名称；

“CertType”： 证书类型；SM2 或 RSA。

“IssuerDN”： 颁发者 DN。

BSTR* pbstrInfoContent: [OUT， RETVAL] 成功返回获取到的信息，失败返回空。

3.3.3 EncryptMsgCMSEnvelopeEx

HRESULT EncryptMsgCMSEnvelopeEx（BSTR bstrMessage, BSTR bstrEncryptAlg, BSTR* pbstrEnvelope）

描述:

使用 SelectEncryptCertificate 选择的 SM2/RSA 公钥证书将消息加密成 CMS 数字信封。

对字符串进行 SM2/RSA 加密，返回 Base64 编码的 SM2/RSA 加密结果；

其中 RSA 签名可以使用 3DES 或 RC4 算法加密，SM2 签名使用 SM4 算法加密。

此函数用于基于 USBKey 的加密。

参数:

BSTR bstrMessage: [IN] 待加密的字符串,(加密之前内部会将其转换为 UTF-8 编码)。

BSTR bstrEncryptAlg:[IN] 加密算法。传入“RC4”或“3DES”，不区分大小写。此参数只对 RSA 证书起作用，SM2 证书默认使用 SM4 算法加密。

BSTR * pbstrEnvelope: [OUT，RETVAL] 加密后的数字信封，Base64 编码格式字符串。

3.3.4 EncryptMsgCMSEnvelopeEx_ByCert

HRESULT EncryptMsgCMSEnvelopeEx_ByCert（BSTR bstrBase64CertContent , BSTR bstrCertType,BSTR bstrMessage, BSTR bstrEncryptAlg, BSTR* pbstrEnvelope）

描述:

使用传入的 SM2/RSA 公钥证书，将消息加密成 CMS 数字信封。

参数:

BSTR bstrBase64CertContent: [IN] SM2/RSA 公钥证书，该证书需采用 Base64 编码。

BSTR bstrCertType:[IN]用于加密公钥证书类型。SM2、RSA。

BSTR bstrMessage: [IN]待加密的字符串，（加密之前内部会将其转换为 UTF-8 编码）。

BSTR bstrEncryptAlg:[IN] 加密算法。传入“RC4”或“3DES”，不区分大小写。此参数只对 RSA 证书起作用，SM2 证书默认使用 SM4 算法加密。

BSTR* pbstrEnvelope: [OUT，RETVAL] 加密后的数字信封，Base64 编码格式字符串。

3.3.5 DecryptMsgCMSEnvelopeEx

HRESULT DecryptMsgCMSEnvelopeEx （ BSTR bstrEnvelope,BSTR bstrEnvelopeType,BSTR* pbstrMessage）

描述:

使用 SelectEncryptCertificate 函数选择的 SM2/RSA 证书解密 CMS 数字信封。

参数:

BSTR bstrEnvelope: [IN] 用于解密的数字信封，Base64 编码格式字符串。

BSTR bstrEnvelopeType:[IN]用于解密的证书类型。SM2、RSA 证书。

BSTR* pbstrMessage: [OUT， RETVAL]解密出的明文字符串。

3.3.6 DecryptMsgCMSEnvelopeEx_BySoftCert

HRESULT DecryptMsgCMSEnvelopeEx_BySoftCert（BSTR bstrSoftCertFileName，BSTR bstrSoftCertPassword, BSTR bstrEnvelope, BSTR bstrEnvelopeType,BSTR* pbstrMessage）

描述:

使用传入的 SM2/RSA 文件证书解密 CMS 数字信封。

参数:

BSTR bstrSoftCertFileName: [IN] 用于解密的 SM2/PFX 文件证书。

BSTR bstrSoftCertPassword: [IN] 用于解密的 SM2/PFX 文件证书的密码。

BSTR bstrEnvelope: [IN]用于解密的数字信封，Base64 编码格式字符串。

BSTR bstrEnvelopeType:[IN]用于解密的证书类型。SM2、RSA 证书。

BSTR* pbstrMessage: [OUT， RETVAL] 解密出的明文字符串。

3.4 消息的加密与解密（老国密 C1||C2||C3 标准）

此系列为兼容老的国密标准：C1||C2||C3 而保留，新客户不建议使用。

建议使用 2.4 中带 Ex 的接口。

3.4.1 EncryptMsgCMSEnvelope

HRESULT EncryptMsgCMSEnvelope（BSTR bstrMessage, BSTR bstrEncryptAlg, BSTR* pbstrEnvelope）

描述:

使用 SelectEncryptCertificate 选择的 SM2/RSA 公钥证书将消息加密成 CMS 数字信封。

对字符串进行 SM2/RSA 加密，返回 Base64 编码的 SM2/RSA 加密结果；其中 RSA 签名可以使用 3DES 或 RC4 算法加密，SM2 签名使用 SM4 算法加密。

此函数用于基于 USBKey 的加密。

参数:

BSTR bstrMessage: [IN] 待加密的字符串，(加密之前内部会将其转换为 UTF-8 编码)。

BSTR bstrEncryptAlg:[IN] 加密算法。传入“RC4”或“3DES”，不区分大小写。此参数只对 RSA 证书起作用，SM2 证书默认使用 SM4 算法加密。

BSTR * pbstrEnvelope: [OUT，RETVAL] 加密后的数字信封，Base64 编码格式字符串。

3.4.2 EncryptMsgCMSEnvelope_ByCert

HRESULT EncryptMsgCMSEnvelope_ByCert（BSTR bstrBase64CertContent , BSTR bstrCertType,BSTR bstrMessage, BSTR bstrEncryptAlg, BSTR* pbstrEnvelope）

描述:

使用传入的 SM2/RSA 公钥证书，将消息加密成 CMS 数字信封。

此接口中对称密钥的加密格式为：C1||C2||C3。

参数:

BSTR bstrBase64CertContent: [IN] SM2/RSA 公钥证书，该证书需采用 Base64 编码。

BSTR bstrCertType:[IN]用于加密公钥证书类型。SM2、RSA。

BSTR bstrMessage: [IN]待加密的字符串，（加密之前内部会将其转换为 UTF-8 编码）。

BSTR bstrEncryptAlg:[IN] 加密算法。传入“RC4”或“3DES”，不区分大小写。此参数只对 RSA 证书起作用，SM2 证书默认使用 SM4 算法加密。

BSTR* pbstrEnvelope: [OUT，RETVAL] 加密后的数字信封，Base64 编码格式字符串。

3.4.3 DecryptMsgCMSEnvelope

HRESULT DecryptMsgCMSEnvelope（ BSTR bstrEnvelope,BSTR bstrEnvelopeType,BSTR* pbstrMessage）

描述:

使用 SelectEncryptCertificate 函数选择的 SM2/RSA 证书解密 CMS 数字信封。

此接口中对称密钥的加密格式为：C1||C2||C3。

参数:

BSTR bstrEnvelope: [IN] 用于解密的数字信封，Base64 编码格式字符串。

BSTR bstrEnvelopeType:[IN]用于解密的证书类型。SM2、RSA 证书。

BSTR* pbstrMessage: [OUT，RETVAL]解密出的明文字符串。

3.4.4 DecryptMsgCMSEnvelope_BySoftCert

HRESULT DecryptMsgCMSEnvelope_BySoftCert（BSTR bstrSoftCertFileName，BSTR bstrSoftCertPassword, BSTR bstrEnvelope, BSTR bstrEnvelopeType,BSTR* pbstrMessage）

描述:

使用传入的 SM2/RSA 文件证书解密 CMS 数字信封。

此接口中对称密钥的加密格式为：C1||C2||C3。

参数:

BSTR bstrSoftCertFileName: [IN] 用于解密的 SM2/PFX 文件证书。

BSTR bstrSoftCertPassword: [IN] 用于解密的 SM2/PFX 文件证书的密码。

BSTR bstrEnvelope: [IN]用于解密的数字信封，Base64 编码格式字符串。

BSTR bstrEnvelopeType:[IN]用于解密的证书类型。SM2、RSA 证书。

BSTR* pbstrMessage: [OUT，RETVAL] 解密出的明文字符串。

3.5 文件的加密与解密

.com、.exe、.bat、.cmd、.vbs、.vbe、.js、.jse、.wsf、.wsh、.msc、.dll 格式文件均不可进行签名及加密操作。

3.5.1 EncryptFileCMSEnvelopeEx

HRESULT EncryptFileCMSEnvelopeEx（BSTR bstrSourceFile, BSTR bstrEncryptAlg, BSTR bstrEncryptedFile, VARIANT_BOOL* pbSuccess）

描述:

使用 SelectEncryptCertificate 选择的 SM2/PFX 公钥证书将文件加密成 CMS 数字信封。

此函数用于基于 USBKey 的加密。

参数:

BSTR bstrSourceFile: [IN] 待加密的文件。

BSTR bstrEncryptAlg: [IN] 加密算法。传入“RC4”或“3DES”，不区分大小写。此参数只对 RSA 证书起作用，SM2 证书默认使用 SM4 算法加密。

BSTR bstrEncryptedFile: [IN] 加密后的文件输出路径(CMS 数字信封)。

VARIANT_BOOL* pbSuccess: [OUT，RETVAL]加密是否成功，VARIANT_TRUE: 加密成功， VARIANT_FALSE: 加密失败。

3.5.2 EncryptFileCMSEnvelopeEx_ByCert

HRESULT EncryptFileCMSEnvelopeEx_ByCert （ BSTR bstrBase64CertContent, BSTR bstrCertType,BSTR bstrSourceFile, BSTR bstrEncryptAlg,BSTR bstrEncryptedFile， VARIANT_BOOL* pbSuccess）

描述:

使用传入的 SM2/PFX 公钥证书，将文件加密成 CMS 数字信封。

参数:

BSTR bstrBase64CertContent: [IN]] SM2/RSA 公钥证书，该证书需采用 Base64 编码。

BSTR bstrCertType:[IN]用于加密公钥证书类型。SM2、RSA。

BSTR bstrSourceFile: [IN] 待加密的文件。

BSTR bstrEncryptAlg: [IN] 加密算法。传入“RC4”或“3DES”，不区分大小写。此参数只对 RSA 证书起作用，SM2 证书默认使用 SM4 算法加密。

BSTR bstrEncryptedFile: [IN] 加密后的数字信封文件输出路径。

VARIANT_BOOL* pbSuccess: [OUT，RETVAL]加密是否成功，VARIANT_TRUE: 加密成功， VARIANT_FALSE: 加密失败。

3.5.3 DecryptFileCMSEnvelopeEx

HRESULT DecryptFileCMSEnvelopeEx （ BSTR bstrEncryptedFile ， BSTR bstrEnvelopeType，BSTR bstrPlainTextFile, VARIANT_BOOL* pbSuccess）

描述:

使用 SelectEncryptCertificate 函数选择的 SM2/PFX 证书解密 CMS 数字信封文件。

参数:

BSTR bstrEncryptedFile: [IN] 用于解密的的数字信封文件。

BSTR bstrEnvelopeType:[IN] 用于解密的证书类型。SM2、RSA 证书。

BSTR bstrPlainTextFile: [IN] 解密出的明文文件。

VARIANT_BOOL* pbSuccess: [OUT，RETVAL]解密是否成功，VARIANT_TRUE: 解密成功，VARIANT_FALSE: 解密失败。

3.5.4 DecryptFileCMSEnvelopeEx_BySoftCert

HRESULT DecryptFileCMSEnvelopeEx_BySoftCert（BSTR bstrSoftCertFileName，BSTR bstrSoftCertPassword, BSTR bstrEncryptedFile, BSTR bstrEnvelopeType,BSTR bstrPlainTextFile, VARIANT_BOOL* pbSuccess）

描述:

使用传入的 SM2/PFX 文件证书解密 CMS 数字信封文件。

参数:

BSTR bstrSoftCertFileName: [IN] 用于解密的 SM2/PFX 文件证书。

BSTR bstrSoftCertPassword: [IN] 用于解密的 SM2/PFX 文件证书的密码。

BSTR bstrEncryptedFile: [IN] 用于解密的数字信封文件。

BSTR bstrEnvelopeType:[IN] 用于解密的证书类型。SM2、RSA 证书。

BSTR bstrPlainTextFile: [IN]解密出的明文文件输出路径。

VARIANT_BOOL*pbSuccess:[OUT，RETVAL] 解密是否成功，VARIANT_TRUE: 解密成功，VARIANT_FALSE: 解密失败。

3.6 文件的加密与解密（老国密 C1||C2||C3 标准）

此系列为兼容老的国密标准：C1||C2||C3 而保留，新客户不建议使用。

建议使用 2.6 中带 Ex 的接口。

.com、.exe、.bat、.cmd、.vbs、.vbe、.js、.jse、.wsf、.wsh、.msc、.dll 格式文件均不可进行签名及加密操作。

3.6.1 EncryptFileCMSEnvelope

HRESULT EncryptFileCMSEnvelope（BSTR bstrSourceFile, BSTR bstrEncryptAlg, BSTR bstrEncryptedFile, VARIANT_BOOL* pbSuccess）

描述:

使用 SelectEncryptCertificate 选择的 SM2/PFX 公钥证书将文件加密成 CMS 数字信封。

此函数用于基于 USBKey 的加密。

参数:

BSTR bstrSourceFile: [IN] 待加密的文件。

BSTR bstrEncryptAlg: [IN] 加密算法。传入“RC4”或“3DES”，不区分大小写。此参数只对 RSA 证书起作用，SM2 证书默认使用 SM4 算法加密。

BSTR bstrEncryptedFile: [IN] 加密后的文件输出路径(CMS 数字信封)。

VARIANT_BOOL* pbSuccess: [OUT，RETVAL]加密是否成功，VARIANT_TRUE: 加密成功， VARIANT_FALSE: 加密失败。

3.6.2 EncryptFileCMSEnvelope_ByCert

HRESULT EncryptFileCMSEnvelope_ByCert（BSTR bstrBase64CertContent, BSTR bstrCertType,BSTR bstrSourceFile, BSTR bstrEncryptAlg,BSTR bstrEncryptedFile，VARIANT_BOOL* pbSuccess）

描述:

使用传入的 SM2/PFX 公钥证书，将文件加密成 CMS 数字信封。

参数:

BSTR bstrBase64CertContent: [IN]] SM2/RSA 公钥证书，该证书需采用 Base64 编码。

BSTR bstrCertType:[IN]用于加密公钥证书类型。SM2、RSA。

BSTR bstrSourceFile: [IN] 待加密的文件。

BSTR bstrEncryptAlg: [IN] 加密算法。传入“RC4”或“3DES”，不区分大小写。此参数只对 RSA 证书起作用，SM2 证书默认使用 SM4 算法加密。

BSTR bstrEncryptedFile: [IN] 加密后的数字信封文件输出路径。

VARIANT_BOOL* pbSuccess: [OUT，RETVAL]加密是否成功，VARIANT_TRUE: 加密成功， VARIANT_FALSE: 加密失败。

3.6.3 DecryptFileCMSEnvelope

HRESULT DecryptFileCMSEnvelope（ BSTR bstrEncryptedFile， BSTR bstrEnvelopeType，BSTR bstrPlainTextFile, VARIANT_BOOL* pbSuccess）

描述:

使用 SelectEncryptCertificate 函数选择的 SM2/PFX 证书解密 CMS 数字信封文件。

参数:

BSTR bstrEncryptedFile: [IN] 用于解密的的数字信封文件。

BSTR bstrEnvelopeType:[IN] 用于解密的证书类型。SM2、RSA 证书。

BSTR bstrPlainTextFile: [IN] 解密出的明文文件。

VARIANT_BOOL* pbSuccess: [OUT，RETVAL]解密是否成功，VARIANT_TRUE: 解密成功，VARIANT_FALSE: 解密失败。

3.6.4 DecryptFileCMSEnvelope_BySoftCert

HRESULT DecryptFileCMSEnvelope_BySoftCert（BSTR bstrSoftCertFileName，BSTR bstrSoftCertPassword, BSTR bstrEncryptedFile, BSTR bstrEnvelopeType,BSTR bstrPlainTextFile, VARIANT_BOOL* pbSuccess）

描述:

使用传入的 SM2/PFX 文件证书解密 CMS 数字信封文件。

参数:

BSTR bstrSoftCertFileName: [IN] 用于解密的 SM2/PFX 文件证书。

BSTR bstrSoftCertPassword: [IN] 用于解密的 SM2/PFX 文件证书的密码。

BSTR bstrEncryptedFile: [IN] 用于解密的数字信封文件。

BSTR bstrEnvelopeType:[IN] 用于解密的证书类型。SM2、RSA 证书。

BSTR bstrPlainTextFile: [IN]解密出的明文文件输出路径。

VARIANT_BOOL*pbSuccess:[OUT，RETVAL] 解密是否成功，VARIANT_TRUE: 解密成功，VARIANT_FALSE: 解密失败。

3.7 其他

3.7.1 SetSM2CSPList

HRESULT SetSM2CSPList（BSTR bstrSM2CSPList）

描述:

设置 SM2 证书所在 CSP 列表。

在进行 SM2 证书选择或 SM2 数字信封解密前，必须调用此接口，以设置用于过滤 SM2 证书的 CSP 列表。

控件加载后，若 CSP 列表不需变更，则只需调用一次即可。

参数:

BSTR bstrSM2CSPList: [IN] 支持 SM2 非注册证书的 CSP 列表。

3.7.2 GetLastErrorDesc

HRESULT GetLastErrorDesc（BSTR* pbstrErrorDesc）

描述:

获得最近一次调用接口导致发生错误的描述信息。此函数会根据不同的操作系统语言（简体中文/美国英语）来本地化错误描述。

参数:

BSTR* pbstrErrorDesc: [OUT， RETVAL]错误描述信息。

4 示例代码

见 Demo 程序。